**ZP/39/2024**  Puławy, dn. 15.03.2024 r.

**ZAPYTANIE OFERTOWE**

**„Zakup licencji na program typu Endpoint Protection/Security”**

1. **ZAMAWIAJĄCY**

Puławski Park Naukowo-Technologiczny Sp. z o.o. z siedzibą ul. Ignacego Mościckiego 1, 24-110 Puławy, reprezentowany przez Tomasza Szymajdę – Prezesa Zarządu

Tel. (81) 464-63-16,

Internet: [ppnt.pulawy.pl](http://www.ppnt.pulawy.pl)

e-mail: biuro@ppnt.pulawy.pl

BIP: <https://ppntpulawy.bip.lubelskie.pl>

1. **OPIS PRZEDMIOTU ZAMÓWIENIA**
2. Rodzaj zamówienia: Usługa.
3. Oznaczenie wg Wspólnego Słownika Zamówień CPV: 48730000-4.
4. Przedmiotem zamówienia jest zakup **licencji na program typu Endpoint Protection/Security. Licencja do użytku komercyjnego na 3 lata.** Zamawiający nie dopuszcza zakupu licencji na krótsze okresy, których łączny okres licencjonowania byłby równy 3 lata.
5. Zamawiający dopuszcza zakup minimum **115 identycznych licencji jeśli producent w swoim rozwiązaniu nie zastosuje rozróżnienia osobno na licencje dla urządzeń niemobilnych i mobilnych**.
6. Początek okresu obowiązywania licencji nie może zaczynać się wcześniej niż dzień poinformowania Wykonawcy o wyborze jego oferty i nie później niż 7 dni po tym dniu.
7. Okres obowiązywania wszystkich licencji musi być jednakowy z dokładnością do jednego dnia.
8. Wszystkie licencje na oprogramowanie, samo oprogramowanie i jego moduły, wtyczki, rozszerzenia, dodatki itp. muszą być ze sobą kompatybilne, w szczególności pod kątem wzajemnej wymiany danych i współpracy oraz w celu realizacji funkcjonalności opisanych w szczegółowej specyfikacji przedmiotu zamówienia.
9. Wszystkie aplikacje wchodzące w skład Przedmiotu zamówienia w tym także jego moduły, wtyczki, rozszerzenia, dodatki itp. powinny być udostępniane bez dodatkowych opłat przez jednego producenta i należeć do jego jednego, spójnego rozwiązania Endpoint Protection/Security.
10. W całym okresie obowiązywania licencji użytkownik ma mieć prawo do korzystania z bezpłatnej pomocy technicznej producenta Przedmiotu zamówienia świadczonej za pośrednictwem telefonu i poczty elektronicznej.
11. **Urządzenia niemobilne - Ilość licencji na min. 105 urządzeń.**
12. **Obsługa systemów operacyjnych minimum:**
	1. **System operacyjny Windows:**
		1. **Systemy Operacyjne Komputerów**

Pełne wsparcie dla Windows 7 SP1 i nowszych.

* + 1. **Windows Tablet oraz systemy wbudowane**

Pełne wsparcie dla:

Windows 10 IoT Enterprise

Windows Embedded 8.1 Industry

Windows Embedded 8 Standard

Windows Embedded 7 Standard, Compact, POSReady, Enterprise

* + 1. **Systemy operacyjne serwera**

Pełne wsparcie dla:

Windows Server 2008 R2 i nowszych włącznie z wariantami „Core”

* 1. **Systemy Operacyjne Linux i wersja kernel**
		1. Oparte o RPM:

RHEL 7.x - 3.10.0 (od buildu 957)

RHEL 8.x - 4.18.0

RHEL 9x - 5.14.0

Oracle Linux 7.x (UEK +RHCK) - 3.10.0-957 - 4.18.0

Oracle Linux 8.x (UEK +RHCK) - 3.10.0-957 - 4.18.0

Oracle Linux 8.x (UEK +RHCK) – 5.15.0

CentOS 7.x - 3.10.0 (od buildu 957)

CentOS 8 Stream - 4.18.0

CentOS 9 Stream - 5.14.0

Fedora 31 – 36 – do czasu wygaśnięcia wsparcia

AlmaLinux 8.x - 4.18.0

AlmaLinux 9.x - 5.14.0

Rocky Linux 8.x - 4.18.0

Rocky Linux 9.x - 5.14.0

CloudLinux 8.x - 4.18.0

CloudLinux 7.x - 3.10

Miracle 8.4 - 4.18.0

* + 1. Oparte o Debian:

Debian 9 - 4.9.0

Debian 10 - 4.19

Debian 11 - 5.10

Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15

Ubuntu 18.04.x - 5.0 / 5.3 / 5.4

Ubuntu 20.04.x - 5.4

Ubuntu 21.10.x - 5.13

Ubuntu 22.04.x - 5.15

PopOS 22.04.x – 6.2

Pardus 21 – 5.10

Mint 20.3 – 5.4.0

Mint 21 – 5.15.0

* + 1. Oparte o SUSE:

SLES 12 SP4 - 4.12.14-x

SLES 12 SP5 - 4.12.14-x

SLES 15 SP1 - 4.12.14-x

SLES 15 SP2 - 5.3.18-x

SLES 15 SP3 - 5.3.18-x

SLES 15 SP4 – 5.14.21

openSUSE Leap 15.2 - 15.4 - 5.3.18 / 5.14.x

* + 1. Cloud based Linux:

AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x

Amazon Linux v2 - 4.14.x / 4.19.x, 5.10

Amazon Linux 2023 – 6.1.x

Google COS - 4.19.112 / 5.4.49

Milestones 77, 81, 85 - 4.19.112 / 5.4.49

Azure Mariner 2 - 5.15

* 1. **Systemy Operacyjne Mac OS X**

macOS Ventura (13.x)

macOS Monterey (12.x)

macOS Big Sur (11.x)

macOS Catalina (10.15)

macOS Mojave (10.14)

1. **Obsługa środowisk Microsoft Exchange**
2. Exchange Server 2019 z rolą Edge Transport lub Mailbox
3. Exchange Server 2016 z rolą Edge Transport lub Mailbox
4. Exchange Server 2013 z rolą Edge Transport lub Mailbox
5. Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox

Wymagana kompatybilność z Microsoft Exchange Database Availability Groups (DAG).

1. **Ochrona środowisk wirtualnych**
	1. Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej.
	2. Maszyna wirtualna pełniąca rolę silnika skanującego powinna być możliwa do pobrana w formatach:

a) OVA

b) XVA

c) VHD

d) VMDK

* 1. Wsparcie dla środowisk:

VMware vSphere i vCenter Server: v 6.5; v 6.7 włącznie z update 1, update 2a i update 3; v 7.0 włącznie z update 1, update 2, update 2b, update 2c i update 2d

VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x

VMware Workstation 11.x, 10.x, 9.x, 8.0.6

VMware Player 7.x, 6.x, 5.x

Citrix Xen Hypervisor: 7.1 (z hotfixem XS71ECU2060), 8.2.

Citrix Virtual Apps and Desktops 7 1808, 1811, 1903 i 1906

Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR

Citrix VDI-in-a-Box 5.x

Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 lub Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (włącznie z Hyper-V Hypervisor)

Red Hat Enterprise Virtualization 3.0 (włącznie z KVM Hypervisor)

Oracle VM 3.0

Oracle VM VirtualBox 5.2, 5.1

Nutanix Prism z AOS 5.6, 5.5, 5.20 LTS, 5.18 STS, 5.15 LTS, 5.11, 5.10 (Enterprise Edition)

Nutanix Prism z AHV 20170830.115, 20170830.301, 20170830.395 i 20190916.294 (Community Edition)

1. **Ochrona antywirusowa i antyspyware:**
2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.
4. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi.
5. Powiadomienia z modułu sprawdzającego procesy wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane mają być również przesyłane za pośrednictwem Syslog.
6. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
7. Wbudowana technologia do ochrony przed rootkitami.
8. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
9. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie”.
10. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
12. Skanowanie plików spakowanych i skompresowanych.
13. Możliwość dodawania wykluczeń na podstawie:
14. Plik
15. Folder
16. Rozszerzenie
17. Proces
18. Hash pliku
19. Hash certyfikatu
20. Nazwa zagrożenia
21. Wiersz poleceń
22. IP/maska
23. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.
24. Skanowanie i oczyszczanie poczty przychodzącej POP3 „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
25. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
26. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch powinien być automatycznie blokowany a użytkownikowi wyświetlane stosowne powiadomienie.
27. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo powinny być zdefiniowane przez producenta grupy stron.
28. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
29. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
30. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
31. Możliwość przechowywania zawartości kwarantanny maksymalnie 180 dni.
32. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH.
33. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki www lub programy pocztowe.
34. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o swoje hasło.
35. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji: „O programie” powinna być możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora pomocy, numer telefonu do administratora pomocy.
36. W GUI programu na punkcie końcowym powinna być możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
37. W GUI programu powinna być możliwość wyświetlenia którego dnia była przeprowadzana ostatnia aktualizacja z dokładnością co do sekundy jej uruchomienia.
38. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
39. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
40. Praca programu musi być niezauważalna dla użytkownika.
41. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania powinien być bezpośrednio na stacji roboczej.
42. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci komputerowej.
43. Oprogramowanie klienckie musi posiadać wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
44. Możliwość odblokowania ustawień programu po wpisaniu hasła.
45. Oprogramowanie musi posiadać możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu.
46. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie).
47. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu.
48. Funkcja ochrony danych ma umożliwiać blokowanie wysyłanych przez http lub smtp danych takich jak: adresy e-mail, piny, konta bankowe, hasła itp.
49. Funkcja ochrony danych ma mieć możliwość konfigurowana zdalnie przez administratora.
50. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
51. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
52. Wbudowany IDS.
53. Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze, lub wykorzystanie dodatkowej maszyny wirtualnej, która przejmie rolę silnika skanującego.
54. Maszyna, która przejmuje rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji.
55. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego.
56. Możliwość tworzenia list sieci zaufanych.
57. Możliwość dezaktywacji funkcji zapory sieciowej.
58. Możliwość ustawienia skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
59. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
60. Mechanizm, który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji.
61. Użytkownik na punkcie końcowym ma mieć możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa).
62. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups.
63. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
64. System zarządzania ryzykiem zintegrowany z konsolą zarządzającą systemem, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:
65. Funkcję, która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:

- Ochrony przeglądarki internetowej;

- Sieć i poświadczenia;

- Błędna konfiguracja systemu operacyjnego.

System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.

1. System zarządzania ryzykiem, który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.
2. System, który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.
3. System, który pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.
4. System, który pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.
5. System, który pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie.
6. Dla systemów Windows wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik ich wykrycia z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja ta powinna umożliwiać również:
7. wymuszenie funkcji DEP,
8. wymuszenie relokacji modułów (ASLR).
9. Ochrona przed atakami sieciowymi tj. mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak:
10. wczesny dostęp
11. dostęp do poświadczeń
12. wykrycie
13. crimeware
14. Ochrona przed ransomware ma mieć możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.

Formaty plików jakie mogą być odzyskane:

3fr, ai, arw, bay, cab, cdr, cer, cr2, crt, crw, dcr, der, dgn, dll, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, exe, indd, ini, jpe, jpeg, jpg, mdf, mef, mrw, msg, msi, nef, nrw, odb, odc, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pdf, pef, pem, pfx, png, ppt, pptm, pptx, psd, pst, ptx, py, r3d, raf, rtf, rw2, rwl, sr2, srf, srw, tsf, wb2, wpd, wps, x3f, xlk, xls, xlsb, xlsm, xlsx, xml.

Oprogramowanie powinno dawać możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania.

1. Ochrona proaktywna oparta o maszynowe uczenie, która działa w fazie poprzedzającej wykonanie. Ochrona ta musi wykrywać zagrożenia takie jak:
2. ukierunkowane ataki
3. podejrzane pliki i ruch w sieci
4. exploity
5. ransomware
6. grayware
7. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego.
8. Moduł ochrony proaktywnej musi działać w trybach, które administrator może dowolnie zmieniać na:
9. tolerancyjny
10. normalny
11. agresywny
12. Zintegrowany sandbox po stronie producenta, który pozwala na analizę pliku:
13. Plik może zostać wysłany automatycznie ze stacji roboczej jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora;
14. Możliwość przesłania archiwum zabezpieczonego hasłem;
15. Możliwość przesłania adresu URL;
16. W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.
17. Wbudowany sandbox musi działać w trybie monitorowania i blokowania.
18. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny.
19. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości, która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania.
20. Wbudowany sandbox musi posiadać opcję, która pozwala na dodanie określonych rozszerzeń do wyjątków. Pliki z tym rozszerzeniem nie powinny być przesyłane do sandboxa.
21. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa to 50MB.
22. Telemetria tj. możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk (wymaga TLS 1.2 lub wyższego).
23. Oprogramowanie powinno zawierać monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
24. Produkt oraz sygnatury muszą być aktualizowane nie rzadziej niż raz na godzinę.
25. Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych.
26. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
27. Program musi posiadać możliwość skanowania jedynie nowych i niezmienionych plików.
28. Program musi umożliwiać określenie jak długo mają być przechowywane zdarzenia na stacji roboczej.
29. Dla maszyn z systemem Linux ma być możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.
30. Po instalacji oprogramowania antywirusowego nie powinno być wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
31. Aktywacja modułu kontroli urządzeń nie powinna wymagać restartu stacji roboczej.
32. **Maszyny Wirtualne**
33. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: strona pomocy, adres e-mail, numer telefonu.
34. Możliwość określenia jak długo mają być przechowywane zdarzenia na stacji roboczej.
35. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem.
36. Wersja kliencka nie powinna pełnić roli ochrony antywirusowej, lecz być tylko agentem dla serwera ochrony.
37. Dla maszyn z systemem Linux możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.
38. Możliwość wskazania do jakiego serwera ochrony maja się łączyć klienci maszyn wirtualnych.
39. **Ochrona Exchange**
40. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
41. Rozwiązanie musi wspierać skanowanie „na życzenie” oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko e-maili z załącznikami bądź e-maili otrzymanych w przeciągu ostatnich godzin czy dni.
42. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz niemożliwych do przeskanowania.
43. Możliwość wykluczenia potencjalnie niechcianych aplikacji z filtrowania antymalware.
44. Możliwość skanowania w poszukiwaniu malware wewnątrz archiwów.
45. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów e-mail i domen.
46. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
47. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.
48. Zdolność do wykonania zapytań bazujących na chmurze dla ochrony przeciw nowemu spamowi.
49. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowania maila do konkretnej skrzynki pocztowej.
50. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.
51. Zdolność do podejmowania różnych akcji na e-mailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie e-maila do konkretnej skrzynki.
52. **Konsola zdalnej administracji On-premise na lokalnym serwerze administracyjnym**
53. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
54. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci komputerowej z jednego serwera zarządzającego.
55. Możliwość integracji wielu domen Active Directory.
56. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
57. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
58. Możliwość utworzenia konta użytkownika z rolą administratora firmy, administratora sieci, analityka bezpieczeństwa lub z ustawieniami niestandardowymi.
59. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej m.in. adresów IP, wersji systemu operacyjnego.
60. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
61. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
62. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.
63. Możliwość uruchomienia centralnej konsoli z poziomu przeglądarki internetowej.
64. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu min. pdf i csv.
65. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.
66. Możliwość generowania raportu co godzinę.
67. Możliwość dodania etykiety do stacji roboczej.
68. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
69. Wykorzystanie bazy danych w serwerze administracyjnym.
70. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.
71. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
72. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie:

- Zakres adresów IP/IP

- Adres bramy

- Adres serwera WINS

- Adres serwera DNS

- Połączenie DHCP sufiksów DNS

- Czy punkt końcowy może rozwiązać hosta

- Typ sieci

- Nazwa hosta

1. Integracja z serwerem Syslog.
2. Możliwość włączenia uwierzytelnienia dwuskładnikowego realizowanego przy pomocy aplikacji kompatybilnej ze standardem RFC6238.
3. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.
4. Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.
5. Funkcja pojedynczego logowania – Single Sign-on (SSO).
6. Możliwość naprawy instalacji z poziomu konsoli.
7. Raport streszczający tj. możliwość podglądu raportu, który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:

- Zarządzane punkty końcowe

- Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze Windows, serwery Windows, macOS, Linux oraz fizyczne punkty końcowe i maszyny wirtualne

- Pięć najczęściej blokowanych zagrożeń

- Podział zagrożeń na urządzenia takie jak stacje robocze i serwery

- Status incydentów bezpieczeństwa które wystąpiły

- Stan modułów punktów końcowych

- Ocena ryzyka firmy

- Zablokowane strony www w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.

- Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware

1. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:
2. Pakiety
3. Sieć
4. Kwarantanna
5. Licencjonowanie
6. Integracje
7. Polityki
8. Raporty
9. Konta
10. Firmy
11. Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta powinna pozwalać również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz pozwala na określenie godziny kiedy te maszyny będą usuwane.
12. Możliwość określenia własnego serwera funkcji kontroli aplikacji.
13. Możliwość integracji z vCenter Server.
14. Możliwość integracji z Xen Server.
15. Możliwość integracji z nutanix Prism Element.
16. Możliwość integracji z Amazon EC2.
17. Możliwość intergracji z Azure.
18. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
19. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.
20. Możliwość określenia profilu przedsiębiorstwa w konsoli administracyjnej jak np. Lotnictwo, Rolnictwo, Automotive, Usługi komercyjne, Doradztwo, Energia, Usługi finansowe, Rząd, Opieka zdrowotna, Technologie, Transport, Non-profit, Górnictwo, Media.
21. Funkcja kontroli aplikacji, która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów.
22. Funkcja kontroli aplikacji powinna móc działać w trybie testowym lub produkcyjnym.
23. Funkcja kontroli aplikacji powinna pozwalać na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat.
24. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
25. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
26. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS.
27. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.
28. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
29. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS.
30. Oprogramowanie powinno umożliwiać pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1.
31. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
32. Oprogramowanie powinno umożliwiać ochronę kontenerów instalowanych bezpośrednio na hoście kontenera oferując wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym.
33. Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Program wczesnego dostępu powinien umożliwiać testowanie najnowszych funkcji oprogramowania, których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.
34. Oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Oprogramowanie musi umożliwiać przypisywanie znaczników ręcznie lub automatycznie. Oprogramowanie musi umożliwiać filtrowanie punktów końcowych na podstawie wybranych znaczników, musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
35. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows.
36. **Endpoint Detection and Response**

Produkt musi zapewniać szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze w tym:

* 1. **Główne elementy:**
1. Czujnik EDR, który gromadzi i przetwarza dane w celu raportowania danych dotyczących punktu końcowego i zachowania aplikacji.
2. Komponent służący do interpretacji metadanych gromadzonych przez czujnik EDR.
3. Możliwość instalacji dodatkowego, lekkiego agenta z czujnikiem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną ochronę. Agent powinien posiadać też ochronę urządzenia i ruchu sieciowego oraz filtr stron internetowych.
	1. **Wykrywanie podejrzanej aktywności**

Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności m.in.:

1. Bazowanie na systemach bazujących na wskaźnikach ataku MITRE i własnej inteligencji.

2. Zgłaszanie wszystkich naruszeń jako incydent w module EDR.

* 1. **Badanie incydentów i wizualizacja**
1. Produkt ma zapewniać wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym przedziale czasu.
2. Produkt ma integrować się z bazą wiedzy ATT & CK firmy MITRE i odpowiednio oznaczać zdarzenia bezpieczeństwa.
3. Produkt ma zapewniać zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi informacjami lub działaniami z następującymi informacjami:
4. Podsumowanie powinno zawierać przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia.
5. Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej.
6. Działania naprawcze gromadzą informacje o działaniach blokujących automatycznie podejmowanych przez produkt w związku z bieżącym zdarzeniem bezpieczeństwa.
	1. **Incydenty**

1. Oprogramowanie ma pozwalać na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz dać możliwość:

a) Filtrowania zdarzeń

b) Blokowania procesów

c) Dodawania procesów do czarnej listy

d) Dodawania procesów do białej listy

e) Izolację hosta

f) Przesłanie pliku do Sandbox

g) Sprawdzenie informacji o pliku w Google

h) Sprawdzenie informacji o pliku w VirusTotal

2. Filtrowanie zdarzeń musi mieć możliwość odbywania się na podstawie:

a) Oceny zagrożenia na podstawie przypisanej ilości punktów

b) Daty wykrycia

c) Statusu

d) ID

e) Nazwy punktu końcowego

f) Typu ataku

g) Ransomware

h) Potencjalnie niechcianej aplikacji

i) Malware

j) Exploit

k) Fileless

l) Password stealer

m) Downloader

n) Innych

o) Zdefiniowanych przez użytkownika

3. Wyszukiwanie zdarzeń może odbywać się na podstawie:

a) Nazwa alertu

b) IP punktu końcowego

c) Hash MD5

d) Hash SHA256

e) Nazwa użytkownika

1. Możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń, które mają najczęściej problem.
2. Możliwość wyświetlenia 10, 20, 30, 50, 100 zdarzeń na jednej stronie.
3. Możliwość wyświetlenia zablokowanych hashy plików.
4. Możliwość dodania własnych hashy MD5 oraz SHA256.
5. Możliwość importu hashy z pliku CSV.
6. Możliwość filtrowania dodanych hashy na podstawie:

a) Typu hashu

b) Wartości hash

c) Źródło dodania

d) Informacje o źródle

e) Nazwa pliku

f) Firma, której dotyczy wpis

1. **Pełne szyfrowanie dysków**
	1. Obsługa systemów operacyjnych minimum:
		1. dla komputerów PC: Windows 7 Enterprise/Ultimate (w tym przypadku Zamawiający dopuszcza rozwiązanie wymagające od Zamawiającego posiadania w systemie modułu TPM), Windows 8/8.1/10 Pro/Enterprise, Windows 11.
		2. dla serwerów: Windows Server 2008 R2 (w tym przypadku Zamawiający dopuszcza rozwiązanie wymagające od Zamawiającego posiadania w systemie modułu TPM), Windows Server 2012 (w tym R2), Windows Server 2016/2019/2022.
		3. dla komputerów Apple z macOS: Sierra (10.12), High Sierra (10.13), Mojave (10.14), Catalina (10.15), Big Sur (11.x), Monterey (12.x).
	2. Cechy i wymagania pełnego szyfrowania dysków:
		1. W systemach Windows szyfrowanie dysków powinno odbywać się z wykorzystaniem natywnej funkcji BitLocker.
		2. W systemach macOS szyfrowanie dysków powinno odbywać się z wykorzystaniem natywnej funkcji FileVault.
		3. Musi być możliwość (de)szyfrowania punktów końcowych poprzez politykę bezpieczeństwa zastosowaną w komputerach.
		4. Musi być możliwość generowania klucza odzyskiwania do funkcji BitLocker z konsoli administracyjnej.
		5. Użytkownik musi ustawić hasło do funkcji szyfrowania zgodnie z ustalonymi wymaganiami.
		6. Licencjonowanie nie może być zależne od ilości dysków w systemie lecz zależeć tylko od ilości (tj. minimum 105 sztuk) systemów operacyjnych.
		7. Funkcja szyfrowania powinna wymagać podania hasła przed odblokowaniem systemu operacyjnego/dysku.
		8. Moduł szyfrowania powinien zapewniać zgodność z wymogami HIPPA, PCI, DSS, GDPR odnośnie szyfrowania danych.
		9. Rozwiązanie nie może wymagać dodatkowego klienta czy serwera do zarządzania modułem szyfrowania.
		10. Administrator musi mieć możliwość ustawienia czy funkcja szyfrująca ma pytać o hasło w momencie uruchamiania systemu operacyjnego z aktywnym modułem TPM.
		11. Musi być możliwość automatycznego zaimportowania klucza odzyskiwania do konsoli administracyjnej po instalacji oprogramowania z modułem szyfrowania, jeżeli urządzenie zostało zaszyfrowane ręcznie przed instalacją tegoż oprogramowania.
		12. Musi być możliwość dodania wyjątków od szyfrowania dla dysków innych niż systemowe.
2. **Urządzenia mobilne - Ilość licencji na min. 10 urządzeń, ochrona urządzeń mobilnych**

**1. Wspierane systemy operacyjne i wymagania**

1. Android w wersji 6 i nowsze przy czym w przypadku urządzeń Knox Zamawiający dopuszcza obsługę systemu Android w wersji 7 i nowszej oraz Knox w wersji 2.7 i nowszej.

2. Apple iOS w wersji 11 i nowszej w tym urządzenia w 64 bitowej wersji.

**2. Cechy ogólne**

Rozwiązanie bezpieczeństwa dla urządzeń mobilnych musi zapewniać co najmniej następujące podstawowe funkcje:

1. Wykrywanie złośliwego oprogramowania.
2. Ochrona przed phishingiem analizująca przychodzące wiadomości i wykrywająca wszelkie złośliwe linki lub treści, które mogą zostać wykorzystane do pozyskania poufnych danych lub poświadczeń.
3. Bezpieczeństwo sieci do ochrony urządzeń mobilnych przed różnymi zagrożeniami sieciowymi. Ta warstwa ochrony powinna zapewniać bezpieczeństwo i integralność urządzeń mobilnych w obecnym stanie zagrożeń poprzez monitorowanie ruchu sieciowego, zapewnianie bezpiecznej łączności oraz wykrywanie i zapobieganie atakom.
4. Zgodność i egzekwowanie zasad jako ochrona urządzeń mobilnych przed różnymi zagrożeniami i zapewnienie, że są one używane bezpiecznie i zgodnie z przepisami, upewniając się, że wszystkie aplikacje są odpowiednio zweryfikowane.
5. Analiza zagrożeń mobilnych zapewniająca użytkownikom zabezpieczenia i analizy w czasie rzeczywistym.
6. Integracja z rozwiązaniami do zarządzania urządzeniami mobilnymi (MDM) w celu zwiększenia bezpieczeństwa mobilnego (np. wymazanie zawartości urządzenia, blokada ekranu).
7. Filtrowanie treści internetowych tj. ostrzeganie i uniemożliwianie użytkownikom dostępu do potencjalnie szkodliwych witryn i linków, takich jak złośliwe oprogramowanie, phishing, botnety i podejrzane domeny lub witryny naruszające standardy organizacji.
8. Możliwość namierzenia lokalizacji urządzenia w momencie wystąpienia incydentu.
9. Funkcja lokalnego VPN na żądanie.

1. **Integracje MDM**

Oprogramowanie powinno obsługiwać integrację z następującymi dostawcami MDM:

- VMWare Workspace ONE UEM MDM

- BlackBerry Dynamics

- BlackBerry's UEM MDM (BES)

- Business Concierge MDM

- Citrix MDM

- MobileIron MDM

- SOTI MobiControl

1. **Integracje SIEM**

Oprogramowanie powinno obsługiwać następujących dostawców SIEM:

- Splunk

- Azure Sentinel

- AT&T AlienVault

- Microsoft Defender ATP

- VMware Workspace ONE Intelligence

1. **Pulpit nawigacyjny**

Oprogramowanie musi zapewniać funkcję pulpitu nawigacyjnego, które zapewnia widok zarządzania wszystkimi urządzeniami:

- Wykres kołowy pokazujący rozkład urządzeń z aktywowaną i chronioną aplikacją, z oczekującymi statusami aktywacji.

- Urządzenia krytyczne - liczba urządzeń z jednym lub więcej zagrożeniami krytycznymi w ciągu ostatnich 90 dni.

- Ryzykowne urządzenia - liczba urządzeń z co najmniej jednym ryzykownym zdarzeniem w ciągu ostatnich 90 dni.

- Ryzyko systemu operacyjnego - urządzenia z systemem Android i iOS, które są podatne na zagrożenia ze względu na przestarzałe i podatne na zagrożenia wersje systemu operacyjnego i muszą zostać zaktualizowane, aby wyeliminować to ryzyko.

- Bieżący wynik bezpieczeństwa - ogólny wynik bezpieczeństwa na wszystkich urządzeniach w oparciu o ocenę aktywacji aplikacji do ochrony urządzeń mobilnych, ryzyka i zagrożeń.

- Trend wyniku bezpieczeństwa - wykres wyświetlany w dziennym, tygodniowym lub miesięcznym przedziale czasowym.

- Kluczowe funkcje - stan włączonych lub wyłączonych kluczowych funkcji aplikacji.

- Możliwość wyświetlania pięciu najważniejszych zagrożeń posortowanych na podstawie liczby zdarzeń z ostatnich 90 dni.

1. **Nasilenie zagrożeń**

Oprogramowanie powinno wskazywać następujące poziomy statusów bezpieczeństwa:

- Krytyczny – wskazuje, że nastąpił rzeczywisty atak lub jest on w trakcie co może oznaczać naruszenie bezpieczeństwa sieci i/lub urządzenia.

- Podwyższony - wskazuje zidentyfikowane ryzyko, które może prowadzić do ataku lub naruszenia bezpieczeństwa sieci lub urządzenia co niekoniecznie oznacza, że doszło do ataku.

- Niski - informacja np. o luce w zabezpieczeniach.

- Normalny – np. w przypadku zdarzeń, takich jak zmiana DNS, zmiana ustawień proxy lub sieci.

**7. Kontrola aplikacji**

1. Oprogramowanie musi obsługiwać weryfikację aplikacji z następującymi ocenami:

- Legalna/Złośliwa - aplikacja lub rozszerzenie jest oceniane na podstawie jej reputacji, autora i dostawców oprogramowania antywirusowego. Jeśli spełnia zalecany próg, jest oceniana jako złośliwa.

- Ryzyko dla prywatności - aplikacja lub rozszerzenie jest oceniane na podstawie zagrożeń dla prywatności, takich jak np. możliwość dostępu do kalendarzy, mikrofonów, lokalizacji.

- Ryzyko bezpieczeństwa - aplikacja jest oceniana na podstawie jej aspektów bezpieczeństwa/kodu w celu zidentyfikowania niebezpiecznych cech aplikacji.

2. Aplikacja może być oznaczona jako:

- Dozwolona

- Odmowa

- Niezgodność

- Brak lub nie dotyczy

**8. Polityka**

1. Polityka wykrywania powinna być skonfigurowana zgodnie z najlepszymi praktykami, z następującymi krytycznymi wątkami domyślnie uwzględnionymi w polityce:

- Jailbreaking/ Rootowanie urządzenia

- Podniesienie uprawnień (EOP)

- MITM (Man-in-the-middle) - Przekierowanie ICMP

- MITM (Man-in-the-middle) - ARP

- Sabotaż systemu

- Nieuczciwy punkt dostępu

- MITM (Man-in-the-middle)

2. Administrator powinien mieć możliwość zmiany poziomów ważności zagrożeń:

- Krytyczny

- Podwyższony

- Niski

- Normalny

3. Akcje urządzenia możliwe do skonfigurowania w Polityce (w zależności od typu wątku):

a) Android i iOS:

- Odłączenie od Wi-Fi: Wyłączenie adaptera Wi-Fi i powrót do danych komórkowych, jeśli są włączone.

- Network Sinkhole: Akcja powinna blokować lub zezwalać na zdefiniowane zakresy sieci/domen w oparciu o skonfigurowaną sieć IP/maskę i domeny.

- Wyłączenie Bluetooth: Wyłącza adapter Bluetooth i rozłącza wszystkie bieżące połączenia Bluetooth.

- Tunelowanie niezabezpieczonego ruchu: Bezpieczny tunel VPN automatycznie inicjowany w celu obsługi ruchu przez niezabezpieczone połączenie.

b) Samsung Knox:

- Wyłączenie/odinstalowanie/zablokowanie aplikacji.

- Odizolowanie od sieci tj. wyłączenie komunikacji sieciowej z aplikacjami, które są złośliwe, ale nie zostały jeszcze odinstalowane.

- Network Sinkhole: Akcja powinna blokować lub zezwalać na zdefiniowane zakresy sieci/domen w oparciu o skonfigurowaną sieć IP/maskę i domeny.

- Zapobieganie utracie danych powinno umożliwiać wymazywanie danych z urządzenia (w tym z karty pamięci).

**9. Zasady dotyczące phishingu i treści internetowych**

1. Ustawienia polityki phishingu i zawartości muszą umożliwiać administratorowi ostrzeganie i ochronę użytkowników przed:

- Uzyskiwaniem dostępu do szkodliwych stron internetowych i linków.

- Uzyskiwaniem dostępu do stron internetowych i linków zawierających treści wymagające działania, takiego jak blokowanie, generowanie zagrożenia, ostrzeganie użytkownika lub kombinacja tych działań.

2. Filtrowanie treści. Rozwiązanie musi obsługiwać dwie główne kategorie treści:

- Kategoria treści Security/Risk musi obejmować następujące podkategorie: Anonymizers, Botnets, Cryptocurrency Mining, Hacking, Illegal Software, Malware, Phishing, Spam, Suspected Domain, Jailbreak/Rooting Tools, Third-Party App Stores.

- Kategoria treści dla dorosłych obejmuje następujące podkategorie: Treści dla dorosłych, Nagość, Pornografia, Edukacja seksualna, Stroje kąpielowe i odzież intymna.

1. **Zagrożenia związane z systemem operacyjnym**

Oprogramowanie musi przedstawiać kompleksowy wykaz wszystkich zidentyfikowanych zagrożeń dla systemów iOS i Android w systemie użytkownika, skategoryzowanych według systemu operacyjnego. Musi zawierać również odpowiednie CVE powiązane z każdym ryzykiem. Musi prezentować:

- Urządzenia z podanym systemem tj. wyświetlać zagregowaną liczbę zagrożonych urządzeń. Dodatkowo zapewniać podział liczby urządzeń z podatnymi wersjami systemu operacyjnego z rozróżnieniem na systemy operacyjne iOS i Android.

- Urządzenia z możliwością aktualizacji tj. wyświetlać łączną liczbę urządzeń, których dotyczy. Dodatkowo musi zapewniać podział liczby na dwie kategorie: urządzenia z systemem iOS i urządzenia z systemem Android, które można zaktualizować.

- Urządzenia bez możliwości aktualizacji tj. wyświetlać łączną liczbę urządzeń, których dotyczy. Dodatkowo musi zapewnić podział liczby urządzeń z systemem iOS i Android, których nie można zaktualizować.

1. **Ustawienia ogólne**

Oprogramowanie musi zawierać, wraz z ogólną konfiguracją produktu, także ustawienia konfiguracji prywatności tj.:

- umożliwiać administratorowi skonfigurowanie typu danych kryminalistycznych, które są gromadzone w przypadku wystąpienia zdarzenia dla każdej zdefiniowanej grupy urządzeń.

- dawać co najmniej dostępny wybór szablonu z następującymi opcjami: Max, High, Medium, Low i Custom (gdzie Low to minimalna ilość danych).

1. **TERMIN WYKONANIA I WARUNKI ROZLICZENIA**
2. Wykonawca zobowiązuje się dostarczyć Zamawiającemu licencje na oprogramowanie zgodnie z treścią Zapytania ofertowego i ofertą Wykonawcy w ciągu 7 dni od dnia otrzymania informacji o wyborze jego oferty.
3. W ciągu 7 dni od otrzymania licencji, o których mowa w ust. 1. Zamawiający dokona weryfikacji ich poprawności oraz zgodności z opisem Przedmiotu zamówienia i ofertą Wykonawcy oraz powiadomi o tym Wykonawcę.
4. Po otrzymaniu przez Wykonawcę informacji od Zamawiającego o przekazaniu prawidłowych licencji Wykonawca ma prawo do dostarczenia Zamawiającemu przelewowej faktury/rachunku za realizację przedmiotu zamówienia, płatnej jednorazowo w terminie minimum 14 dni, w kwocie podanej w ofercie Wykonawcy.
5. W ramach wynagrodzenia oraz z chwilą otrzymania informacji, o których mowa w ust. 3, Zamawiający stanie się licencjobiorcą i użytkownikiem końcowym przedmiotu zamówienia.
6. **OPIS SPOSOBU PRZYGOTOWYWANIA OFERT**
7. Wykonawca może złożyć tylko jedną ofertę, w której musi być zaoferowana tylko jedna cena. Złożenie większej liczby ofert spowoduje odrzucenie wszystkich ofert.
8. Na ofertę składa się - Formularz ofertowy – zał. nr 1 do zapytania ofertowego.
9. Ofertę należy sporządzić w języku polskim zgodnie z treścią załącznika do niniejszego zapytania. Zaleca się jej sporządzenie pismem maszynowym lub komputerowym, ręcznie długopisem lub nieścieralnym atramentem. Powinna być podpisana przez osobę uprawnioną/osoby uprawnione do reprezentowania Wykonawcy.
10. Wszystkie miejsca, w których Wykonawca naniósł zmiany powinny być podpisane przez osobę uprawnioną do występowania w imieniu Wykonawcy wraz z datą naniesienia zmiany.
11. Zamawiający uznaje, że podpisem jest: złożony własnoręcznie naniesiony znak, z którego można odczytać co najmniej nazwisko podpisującego, a jeżeli ten znak jest nieczytelny lub nie zawiera pełnego imienia i nazwiska (podpis skrócony) to znak musi być uzupełniony napisem (np. w formie pieczęci), z którego można odczytać co najmniej imię i nazwisko podpisującego lub elektroniczny podpis kwalifikowany.
12. Cena w ofercie powinna być podana w złotych polskich i obejmować cenę w rozumieniu art. 3 ustawy z 9 maja 2014 r. o informowaniu o cenach towarów i usług. (Dz. U. z 2019 r. poz. 178). Cena oferty powinna być podana w PLN cyfrowo i słownie z zaokrągleniem do dwóch miejsc po przecinku.
13. Cena podana w ofercie powinna obejmować wszystkie koszty i składniki związane z wykonaniem zamówienia oraz z warunkami stawianymi przez Zamawiającego i obejmować cały zakres zamówienia.
14. Cenę należy podać zgodnie z wzorem zawartym w formularzu ofertowym, stanowiącym załącznik nr 1 do niniejszej zapytania.
15. Wszelkie rozliczenia między Zamawiającym a Wykonawcą prowadzone będą w złotych polskich.
16. Zamawiający informuje, że jeżeli zostanie złożona oferta, której wybór prowadziłby do powstania
u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów
i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, ma obowiązek poinformować Zamawiającego, czy wybór oferty będzie prowadzić do powstania
u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.
17. Wykonawca może wprowadzić zmiany lub wycofać ofertę złożoną przed upływem terminu składania ofert.
18. Wykonawcy będą związani swoimi ofertami 30 dni od końca terminu składania ofert.

**V. TERMIN I FORMA SKŁADANIA PROPOZYCJI CENOWYCH.**

* + 1. Termin składania ofert upływa dnia: **25.03.2024 r. do godz. 09:00**
		2. Ofertę można złożyć w jeden z następujących sposobów:
1. W formie elektronicznej poprzez wysyłkę na adres e-mail: **zamowienia@ppnt.pulawy.pl** lub
2. W formie papierowej: osobiście, za pośrednictwem Poczty Polskiej, kuriera, posłańca itp. w sekretariacie Puławskiego Parku Naukowo-Technologicznego, ul. Mościckiego 1, 24-110 Puławy.
3. Za datę złożenia oferty uznaje się datę faktycznego wpływu oferty do Zamawiającego.
4. W przypadku złożenia oferty po terminie określonym w pkt 1 oferta nie będzie rozpatrywana.
5. W przypadku zamiaru złożenia oferty w wersji elektronicznej poprzez wysyłkę na adres mailowy oferta winna był złożona w formie skanu lub zdjęć wypełnionych załączników do zapytania ofertowego lub poprzez wypełnienie ich jedynie komputerowo, przy czym w miejscu na pieczęć Wykonawcy należy wpisać: nazwę i adres Wykonawcy, natomiast w miejscu na podpis wpisać imię i nazwisko osoby/ osób uprawnionych do złożenia oferty. Ofertę można również podpisać kwalifikowanym podpisem elektronicznym.
	* 1. Wykonawca, w przypadku woli zachowania poufności oferty, może:
6. Zamieścić ofertę w wersji papierowej w zamkniętej kopercie. W takim przypadku koperta powinna być zaadresowana na adres Zamawiającego: Puławski Park Naukowo-Technologiczny Sp. z o.o., ul. I. Mościckiego 1, 24-110 Puławy. Ponadto na kopercie należy umieścić w widocznym miejscu i czytelnym drukiem **„ZP/39/2024”**
7. Przesłać ofertą w formie elektronicznej w pliku zaszyfrowanym i niezwłocznie po upływie terminu składania ofert przesłać hasło do otwarcia pliku zawierającego ofertę.
	* 1. Oferty złożone w sposób określony w pkt 6 będą jawne po terminie składania ofert.
		2. W przypadku złożenia oferty z pominięciem zasad poufności określonych w pkt 5 oferty będą jawne przed terminem składania ofert jedynie dla Zamawiającego.
		3. Wykonawca może zmienić lub wycofać swoją ofertę przed terminem składania ofert przez osobę uprawnioną.

**VI. OPIS KRYTERIÓW OCENY OFERT**

1. Kryterium oceny ofert:

**Cena (C) – waga 100%.**

1. Opis sposobu przyznawania punktacji w kryterium: Cena (C).

Kryterium „Cena” będzie rozpatrywane na podstawie ceny brutto za wykonanie przedmiotu zamówienia podanej przez Wykonawcę w formularzu ofertowym. Ilość punktów w tym kryterium zostanie obliczona na podstawie poniższego wzoru:

**C = (Cena brutto oferty najtańszej / Cena brutto oferty badanej) \* 100 pkt**

W ramach tego kryterium można otrzymać maksymalnie 100 pkt.

1. Przyznane punkty zostaną zaokrąglone do dwóch miejsc po przecinku.
2. W przypadku rozbieżności w wyliczeniach ceny netto, podatku VAT i ceny brutto, podstawą do dokonywania poprawek będzie cena netto.
3. W przypadku rozbieżności pomiędzy zapisami cen cyfrowo i słownie podstawą dokonania poprawek będą zapisy cyfrowe.
4. Jeżeli wybór oferty najkorzystniejszej będzie niemożliwy z uwagi na to, że dwie lub więcej ofert uzyska taką samą liczbę punktów, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie przez niego określonym ofert dodatkowych.
5. Wykonawcy składający oferty dodatkowe nie mogą zaoferować wyższych cen jak zaoferowane w złożonych wcześniej ofertach.
6. W przypadku odmowy udzielenia zamówienia przez wybranego Wykonawcę, Zamawiający może zlecić wykonanie przedmiotu zamówienia Wykonawcy, który spełnia wymagania zapytania ofertowego i którego oferta uzyskała kolejno najwyższą ilość punktów.
7. **INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ WYKONAWCY Z ZAMAWIAJĄCYM**
8. W niniejszym zapytaniu ofertowym wszelkie pytania, oświadczenia, wnioski, zawiadomienia oraz informacje dotyczące zapytania ofertowego przekazywane są w formie:
9. drogą elektroniczną na adres: zamowienia@ppnt.pulawy.pl lub
10. papierowej, na adres Zamawiającego:

Puławski Park Naukowo-Technologiczny Sp. z o.o.

ul. Ignacego Mościckiego 1, 24-110 Puławy,

1. Osoba uprawniona do kontaktu z Wykonawcami:
2. W sprawie pytań dotyczących przedmiotu zamówienia: Paweł Szymański, tel. 663 507 602, pawel.szymanski@ppnt.pulawy.pl.
3. W sprawach formalnych: Monika Szarowolec-Chołuj, tel. 606 532 688, monika.choluj@ppnt.pulawy.pl.
4. **INFORMACJA O WYBORZE OFERTY / UNIEWAŻNIENIU POSTĘPOWANIA**
5. O wyborze najkorzystniejszej oferty Zamawiający poinformuje wszystkich wykonawców, którzy złożyli oferty poprzez przesłanie informacji na adres e-mail wskazany w formularzu ofertowym oraz umieści informację na BIP.
6. Zamawiający zastrzega sobie prawo unieważnienia postępowania na każdym jego etapie bez podawania uzasadnienia.
7. **PRZETWARZANIE DANYCH OSOBOWYCH**
8. Wykonawca składając ofertę wyraża zgodę na gromadzenie i przetwarzanie swoich danych osobowych przez Zamawiającego w zakresie niezbędnym do realizacji niniejszej umowy, zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej jako „RODO” lub „Ogólne rozporządzenie o ochronie danych osobowych”). Przetwarzanie powierzonych danych osobowych będzie odbywało się z poszanowaniem przepisów RODO oraz wydanych w związku z nim krajowych przepisów z zakresu ochrony danych osobowych.
9. Zamawiający oświadcza, administratorem danych osobowych jest Puławski Park Naukowo – Technologiczny Sp. z o.o. z siedzibą w Puławach, ul. I. Mościckiego 1, 24-110 Puławy zwany dalej Administratorem. Administrator prowadzi operacje przetwarzania danych osobowych,
10. Zamawiająca oświadcza, iż inspektorem danych osobowych jest wyznaczona przez Administratora osoba, z którą można kontaktować się pocztą elektroniczną na adres e-mail: krzysztof.golaszewski@togatus.pl, telefonicznie na numer 501346042 lub na adres wskazany w punkcie 2.
11. Zamawiający będą przetwarzać dane osobowe wyłącznie w zakresie i celu wykonania umowy oraz realizacji obowiązku prawnego na podstawie art. 6 ust. 1 lit. b i c RODO oraz Ustawy o rachunkowości.
12. Podanie danych osobowych jest warunkiem udziału w postępowaniu, ewentualnego zawarcia umowy oraz wymogiem ustawowym do wypełnienia obowiązków wynikających z mocy prawa. Brak podania danych osobowych uniemożliwia ocenę ofert, zawarcie umowy i prawidłowe jej wykonanie.
13. Dane mogą być udostępniane dostawcom, usługodawcom i partnerom, z którymi Zamawiający podejmuje współpracę w zakresie niezbędnym do realizacji umowy i kontaktów biznesowych. Odbiorcą danych mogą być w szczególności: Puławski Park Naukowo-Technologiczny Sp. z o.o, Instytucje Pośredniczące, Instytucje Zarządzające oraz inne instytucje państwowe i unijne, jak również podmioty zaangażowane przez te instytucje w związku z audytem, rozliczeniem i kontrolą, Urząd Skarbowy, Bank, Kancelaria Prawna, Poczta Polska, firmy kurierskie. Ponadto dane mogą być przekazywane/udostępniane dostawcom i podwykonawcom usług tj. informatyk, biuro rachunkowe, firmy doradczo-konsultingowe – takie podmioty przetwarzają dane tylko na podstawie umowy oraz tylko zgodnie z poleceniami.
14. Dane osobowe nie będą przetwarzane w celu zautomatyzowanego podejmowania decyzji oraz nie będą przekazywane do państw trzecich.
15. Wykonawca posiada prawo do:
16. żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych,
17. wniesienia sprzeciwu wobec takiego przetwarzania,
18. przenoszenia danych,
19. wniesienia skargi do organu nadzorczego.
20. Wykonawcy nie przysługuje:
21. w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
22. prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
23. na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania danych osobowych Wykonawcy jest art. 6 ust. 1 lit. c RODO.
24. Okres przetwarzania obejmuje okres wykonywania zobowiązań oraz okres przedawnienia roszczeń wynikający z przepisów, oraz okres przechowywania dokumentacji.
25. Wykonawcy przysługuje prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie danych osobowych przez administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.
26. **ZAŁĄCZNIKI DO ZAPYTANIA OFERTOWEGO**
27. Formularz cenowy – załącznik nr 1.

**Tomasz Szymajda**

**Prezes zarządu**